The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

02/11/2014

SUBJECT:

Cumulative Security Update for Internet Explorer (MS14-010)

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities could result in an attacker gaining elevated privileges on the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

This advisory covers twenty-three privately disclosed vulnerabilities and one publically disclosed vulnerability (CVE-2014-0267). There has not been any active exploitation or exploit code observed for any of these vulnerabilities at the time of their announcement.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Internet Explorer. The details of these vulnerabilities are as follows:

- One elevation of privilege vulnerability exists in Internet Explorer, caused when Internet Explorer fails to properly validate permissions. This allows an attacker to lure a user to a malicious website, which will elevate the attackers privileges.
- One cross-domain information disclosure vulnerability, caused when Internet Explorer does not properly enforce cross-domain policies. This allows an attacker to view information from another domain or Internet Explorer zone. An attacker can perform this exploit by hosting a malicious website and enticing a user to view it.
- Twenty-two memory corruption vulnerabilities, which occur due to the way Internet Explorer improperly accesses objects in memory. These vulnerabilities could allow an attacker to execute remote code by luring a victim to a malicious website. When the website is visited the attacker’s script will run with same permissions as the affected user.

Successful exploitation of these vulnerabilities could result in an attacker gaining full system privileges on the computer. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.
-

REFERENCES:

Microsoft:

https://support.microsoft.com/kb/2909921

https://technet.microsoft.com/en-us/security/bulletin/ms14-010

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0267

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0268

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0269

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0270

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0271

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0272

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0273

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0274

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0275

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0276

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0277

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0278

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0279

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0280

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0281

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0282

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0283

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0284

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0285

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0286

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0287

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0288

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0289

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0290

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0293